

ABSTRACT

An architecture for secure network communications includes a security layer sandwiched between an upper connection layer and a lower connection layer. An application program need not deal directly with the details of security handshakes, encryption, and decryption. Instead, the application sends plain text data to the upper connection layer, which passes it to the security layer. The security layer manages the necessary security handshakes, and encrypts the data. The security layer then passes the encrypted application data to the lower connection layer, which transports it using TCP or another transport protocol. The security layer need not manage the transport protocol, as this is done by the connection layers. Encrypted data received over the network at the lower connection layer is passed to the security layer for decryption, and then to the upper connection layer for transport to the application.

5021/pc0